10-2009

The tricky business of copying, stealing and protecting

Knowledge@SMU

(http://knowledge.smu.edu.sg)

The tricky business of copying, stealing and protecting

Published: October 02, 2009 in Knowledge@SMU

In 2005, Sony BMG introduced a new line of music compact discs (CD) that contained a unique software application. The Extended Copy Protection (XCP) software, as its name suggests, was a move by the major recording company to combat music piracy by disallowing the copying of music from the discs. Users had to install XCP before they could listen to the music CDs on computers. The introduction of this supplementary yet compulsory application did not deter thousands from purchasing Sony BMG music CDs which they continued to use at home and at work.

Information about XCP had been printed on CD jackets. Terms and conditions of use were also made to appear on computer screens: pop-ups with lengthy text that most consumers would just gloss over at best, or ignore completely. Yet people would be inclined to click "yes" and "agree" so that they could access their music, implying that they have given "permission" for XCP to be installed. So when it was revealed publicly that XCP had left computers vulnerable to security exploits, it was too late. Thousands of computers were affected.

The problem was compounded as each CD could be played on several computers. Home, business and government machines were affected; personal, commercial, national and other sensitive information had been compromised. Many people were upset and civil suits were filed. Several US states, such as Texas, New York and California, also filed criminal prosecutions against Sony BMG.

"So one company, in trying to protect its intellectual property (IP), caused harm to over 500,000 systems in other companies and the government; some in sensitive agencies like the state department, the department of defence and department of homeland security, to have machines that were infected, basically, with holes that caused security problems," Andrea Matwyshyn (http://www.wharton.upenn.edu/faculty/matwyshyn.html) recalled.

The assistant professor of legal studies and business ethics at the University of Pennsylvania's Wharton School observed that Sony BMG had been unapologetic about the nuisance caused. Sony BMG argued that users had clicked "yes" and agreed, contractually, to the software installation. This raises the issue of fair disclosure – do people really know what they are agreeing to when they click "yes"? Was the contract well presented and explained to users? Can users negotiate the terms?

Matwyshyn, who spoke at a recent Wharton-SMU Research Seminar (http://www.smu.edu.sg/centres/wsrc/index.asp), highlighted that there have been gaps in the understanding of information management strategies and norms. Aside from adding to the confusion, knowledge gaps also have wider business implications. "There is a disclosure question, there is a behaviour question and there is a broader question of whether this type of intellectual property protection is desirable or legal, and what this means for a company, in terms of public relations, in choosing how to build its brand, IP and how to market itself."

An end-point to compromise

Information is seen to be the new corporate currency; the trading of information can form a crucial aspect of business. An analyst or management consultant sells her clients information in the form of insights, for instance. A production manager can plan her output better with information, such as demand forecasts. An educator or trainer makes a living out of presenting information to students and executives. Increasingly, organisations are discovering the value of aggregating, packaging, using, managing and licensing information. However, this new line of business presents a new set of challenges – challenges that may not be easily addressed by law.

In 2007, Monster.com, a jobseeker website, experienced a data breach. Millions of users were affected. This was especially aggravating to users (both job applicants and employers) as the information provided within job applications tends to be highly sensitive and personal. Monster.com had been informed about the breach by their security contractor. However, they notified affected users only at the last possible moment, as required by the law (US data breach notification laws) – a move that infuriated customers, companies and the media.

Before the users were notified, hackers had already harvested the data by sending out emails to the Monster.com database masquerading as Monster.com. Customers, unaware about the data compromise, clicked on the links provided by the hackers – links that would then introduce malicious codes into the user's computer. "Monster.com followed the letter of the law but the information was already out there," Matwyshyn said. But how could the laws have allowed such harms?

To prosper in the information age, organisations need to be able to manage and protect their intellectual property. However, Matwyshyn argued that there needs to be a reasonable end-point for permissible measures, so that organisations cannot cause harm to others in the course of IP protection. This end-point can be defined by the financial costs to consumers and companies. "We have a broader problem that goes beyond simply intellectual property protection and gets into the realm of consent and thinking about how to fix the harms that are passed on to others," she said, adding that there is a business ethics dilemma in addition to a legal dilemma.

So what are the norms?

In the commercial world, contracts define and bind relationships. However, the way in which people respond to contracts in the physical space differs greatly from that in the digital space. In the physical space, contracts appear real – it is tangible, you can flip and glance through its pages quite effortlessly. Contracts are also usually presented by a human in the physical space – and as such, terms can be explained and negotiated, person-to-person.

Things are different in the digital space. Contracts appear as static text within a window. Yet, there is no standardisation in appearance as contracts can appear in various forms, based on the size, brightness, and contrast of the machine's display. Formatting may differ across a variety of windows and internet browsers. Fonts can appear differently as well, depending on the display. But worse of all, consumers are expected to accept the contract as it is – wholesale – as there would often be no avenues for interaction or negotiation.

The absence of user-friendly norms or conventions in digital contracting is problematic, according to Matwyshyn. "Notices or terms of use on websites are usually not presented well. How many people really look for the terms of use on websites – many times on 8.5, grey font on grey, at the bottom of a website? Same thing with privacy policies – most people don't read privacy policies! What results is a set of circumstances that doesn't necessarily encourage people to be informed about the code on a website, the code in a CD, the code that they may encounter when they deal with companies who deal with their machines, or what rights are they giving up in their information."

So when people cannot understand, or see no need to understand a contract, they might have a higher tendency to turn in their rights. However, doing so could lead to subsequent problems, as the Sony BMG case clearly illustrates. "Consent, ideally, is a situation where the person who is drafting the contract and the people who are reading the contract have a shared understanding -- everyone knows what is going to happen in the transaction, what code they are interacting with, what is going to occur as a result, and what will happen down the road if something goes wrong with the relationship," said Matwyshyn.

However, this is not the case today. The readers' general indifference towards digital contracts could be due, in part, to an imbalanced relationship with contract authors. The drafter has more leverage today, as readers generally may not question or negotiate contract terms in the digital space.

Matwyshyn believes that a solution could be in balancing the author-reader dynamic. To achieve this, laws could uphold a presumption against the contract drafter – to hold the drafter responsible for ensuring that the contract is understandable to everyone. "This will trigger a greater level of care in contract drafting to focus more on the terms and understanding of contracts rather than one-sided, non-negotiated terms that only favour the drafter," she said. Such a system, she adds, will be good for businesses, as it keeps the drafters up-to-date on what their customers understand and accept. It would also put the contract drafters in a favourable position if they need to defend their contract in courts.

Dumping dollars on the street

While more and more organisations are starting to understand the complexities of information management, Matwyshyn noted that a fundamental gap still exists. Business leaders still perceive IP as a cost that should be minimised – a view that will likely please shareholders in the short term but potentially heighten risks in the long run. As evidenced in past cases to the likes of Monster.com, foul-ups can cost organisations more than just customers – they risk their brand image and they can also stand to lose goodwill with their partners, customers, the public, and ultimately, shareholders.

Matwyshyn raised the idea of inculcating a sense of 'asset sensitive governance' in organisations – thinking beyond the discreet transactions, quarterly numbers and the balance sheet; and paying greater attention to the day-to-day behaviours that could damage the corporate brand, goodwill, and in the long term, to the corporation's intelligence. Unfortunately, laws and business practices today do little to encourage holistic, long-term thinking. Quick, short-term gains are rewarded instead.

So how might organisations correct behaviours that are fundamentally incompatible with good information control practices? Perhaps leaders could be encouraged to think about their fiduciary duties in terms of maximising the value of assets, as opposed to transactional values. Leaders should think for the long haul to see the big, strategic picture. "By having a fiduciary duty set that is thinking about management at every moment in a corporation's history, you start to have a set of corporate decisions that are made with the long term in mind, and not with this quarter's results, because the officers and directors realise that they are not only responsible for this moment in time, but what will happen to the information that they currently have control over, in five years – that it is also

part of their job."

According to Matwyshyn, many organisations are still quite oblivious to the critical importance of information management to the overall success of any business. Nevertheless, there is a heightened sensitivity to this issue because of security laws in some countries, requiring financial officers to monitor the integrity of financial reporting and information security issues. Internal processes and mechanisms aside, companies also need to consider downstream effects to the economy, marketplace, consumers and shareholders.

Decision makers concerned about a business' long-term growth need to consider these issues, especially as digital and information technologies evolve quickly. Matwyshyn concluded, "Until the knowledge gap gets remedied and companies really start to view information as currency – that when you let your information leak out, it's as if you've dumped dollars on the street - until companies start to view information in that way, you're not going to get that kind of prudent management that is necessitated by today's technological circumstances."

back to top (#top)